Amendments to the Claims

Claim 1 (currently amended): In a computing environment having a connection to a network, a computer program product for securely propagating security credentials from a trusted master registry, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for establishing a secure connection between a client and a password synchronization agent (PSA);

computer-readable program code means for transmitting an identifier of a user and an identifying secret of the user from the client to the PSA over the secure connection;

computer-readable program code means for validating the user with the trusted master registry using the transmitted user identifier and identifying secret, on request of the PSA; and

computer-readable program code means for propagating the identifying secret of the user directly from the PSA to one or more target registries if the validation succeeds.

Claim 2 (original): The computer program product according to Claim 1, further comprising:

computer-readable program code means for establishing a second secure connection between the PSA and the trusted master registry; and

computer-readable program code means for using the second secure connection for the validating of the user.

Claim 3 (original): The computer program product according to Claim 1, further comprising:

computer-readable program code means for establishing additional secure connections

between the PSA and each of the target registries; and

computer-readable program code means for using the additional secure connections for the propagating of the identifying secret.

Claim 4 (original): The computer program product according to Claim 1, wherein the master registry stores password synchronization policy information, and wherein the computer-readable program code means for propagating the identifying secret further comprises computer-readable program code means for identifying the target registries using the stored password synchronization policy information for the user.

Claim 5 (original): The computer program product according to Claim 1, wherein the master registry stores password synchronization policy information, and wherein the computer-readable program code means for propagating the identifying secret further comprises computer-readable program code means for identifying the target registries using the stored password synchronization policy information for a user group of which the user is a member.

Claim 6 (original): The computer program product according to Claim 1, wherein the computer-readable program code means for establishing the secure connection further comprises computer-readable program code means for authenticating the PSA to the client.

Claim 7 (original): The computer program product according to Claim 2, wherein the computer-readable program code means for establishing the second secure connection further comprises

computer-readable program code means for authenticating the master registry to the PSA.

Claim 8 (original): The computer program product according to Claim 3, wherein the computer-readable program code means for establishing additional secure connections further comprises computer-readable program code means for authenticating the one or more target registries to the PSA.

Claim 9 (currently amended): The computer program product according to Claim 1, wherein the computer-readable program code means for validating further comprises:

computer-readable program code means for performing a security function on the identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;

computer-readable program code means for using the user identifier to locate a previously-stored identifying secret of the user which was stored by the master registry; and

computer-readable program code means for concluding that the validation succeeds if ~~comparing~~ the located identifying secret is identical to a result of performing the security function.

Claim 10 (original): The computer program product according to Claim 1, wherein the computer-readable program code means for validating further comprises computer-readable program code means for invoking an authenticated LDAP bind or other native authentication mechanism of the master registry, wherein the identifier of the user and the identifying secret of the user are passed to the master registry, thereby causing the master registry to validate the passed identifier and

identifying secret and return a result which reports a success or failure of the validation.

Claim 11 (original): The computer program product according to Claim 1, wherein the PSA has administrative authority for performing operations at the one or more target registries.

Claim 12 (currently amended): The computer program product according to Claim 1, further comprising:

computer-readable program code means for obtaining a new value from the user to be used as the propagated identifying secret if the validation succeeds; and

computer-readable program code means for substituting this new value for the identifying secret prior to operation of the computer-readable program code means for propagating.

Claim 13 (currently amended): A system for securely propagating security credentials from a trusted master registry, comprising:

means for establishing a secure connection between a client and a password synchronization agent (PSA);

means for transmitting an identifier of a user and an identifying secret of the user from the client to the PSA over the secure connection;

means for validating the user with the trusted master registry using the transmitted user identifier and identifying secret, on request of the PSA; and

means for propagating the identifying secret of the user directly from the PSA to one or more target registries if the validation succeeds.

Claim 14 (original): The system according to Claim 13, further comprising:

means for establishing a second secure connection between the PSA and the trusted master registry; and

means for using the second secure connection for the validating of the user.

Claim 15 (original): The system according to Claim 13, further comprising:

means for establishing additional secure connections between the PSA and each of the target registries; and

means for using the additional secure connections for the propagating of the identifying secret.

Claim 16 (original): The system according to Claim 13, wherein the master registry stores password synchronization policy information, and wherein the means for propagating the identifying secret further comprises means for identifying the target registries using the stored password synchronization policy information for the user.

Claim 17 (original): The system according to Claim 13, wherein the master registry stores password synchronization policy information, and wherein the means for propagating the identifying secret further comprises means for identifying the target registries using the stored password synchronization policy information for a user group of which the user is a member.

Claim 18 (original): The system according to Claim 13, wherein the means for establishing the secure connection further comprises means for authenticating the PSA to the client.

Claim 19 (original): The system according to Claim 14, wherein the means for establishing the second secure connection further comprises means for authenticating the master registry to the PSA.

Claim 20 (original): The system according to Claim 15, wherein the means for establishing additional secure connections further comprises means for authenticating the one or more target registries to the PSA.

Claim 21 (currently amended): The system according to Claim 13, wherein the means for validating further comprises:

means for performing a security function on the identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;

means for using the user identifier to locate a previously-stored identifying secret of the user which was stored by the master registry; and

means for concluding that the validation succeeds if ~~comparing~~ the located identifying secret is identical to a result of performing the security function.

Claim 22 (original): The system according to Claim 13, wherein the means for validating further comprises means for invoking an authenticated LDAP bind or other native authentication

mechanism of the master registry, wherein the identifier of the user and the identifying secret of the user are passed to the master registry, thereby causing the master registry to validate the passed identifier and identifying secret and return a result which reports a success or failure of the validation.

Claim 23 (original): The system according to Claim 13, wherein the PSA has administrative authority for performing operations at the one or more target registries.

Claim 24 (currently amended): The system according to Claim 13, further comprising:

means for obtaining a new value from the user to be used as the propagated identifying secret if the validation succeeds; and

means for substituting this new value for the identifying secret prior to operation of the means for propagating.

Claim 25 (currently amended): A method for securely propagating security credentials from a trusted master registry, comprising steps of:

establishing a secure connection between a client and a password synchronization agent (PSA);

transmitting an identifier of a user and an identifying secret of the user from the client to the PSA over the secure connection;

validating the user with the trusted master registry using the transmitted user identifier and identifying secret, on request of the PSA; and

propagating the identifying secret of the user directly from the PSA to one or more target registries if the validation succeeds.

Claim 26 (original): The method according to Claim 25, further comprising steps of:

establishing a second secure connection between the PSA and the trusted master registry; and

using the second secure connection for the validating of the user.

Claim 27 (original): The method according to Claim 25, further comprising steps of:

establishing additional secure connections between the PSA and each of the target registries; and

using the additional secure connections for the propagating of the identifying secret.

Claim 28 (original): The method according to Claim 25, wherein the master registry stores password synchronization policy information, and wherein the step of propagating the identifying secret further comprises the step of identifying the target registries using the stored password synchronization policy information for the user.

Claim 29 (original): The method according to Claim 25, wherein the master registry stores password synchronization policy information, and wherein the step of propagating the identifying secret further comprises the step of identifying the target registries using the stored password synchronization policy information for a user group of which the user is a member.

Claim 30 (original): The method according to Claim 25, wherein the step of establishing the secure connection further comprises the step of authenticating the PSA to the client.

Claim 31 (original): The method according to Claim 26, wherein the step of establishing the second secure connection further comprises the step of authenticating the master registry to the PSA.

Claim 32 (original): The method according to Claim 27, wherein the step of establishing additional secure connections further comprises the step of authenticating the one or more target registries to the PSA.

Claim 33 (currently amended): The method according to Claim 25, wherein the step of validating further comprises:

performing a security function on the identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;

using the user identifier to locate a previously-stored identifying secret of the user which was stored by the master registry; and

concluding that the validation succeeds if ~~comparing~~ the located identifying secret is identical to a result of performing the security function.

Claim 34 (original): The method according to Claim 25, wherein the step of validating further

comprises the step of invoking an authenticated LDAP bind or other native authentication mechanism of the master registry, wherein the identifier of the user and the identifying secret of the user are passed to the master registry, thereby causing the master registry to validate the passed identifier and identifying secret and return a result which reports a success or failure of the validation.

a5

Claim 35 (original): The method according to Claim 25, wherein the PSA has administrative authority for performing operations at the one or more target registries.

Claim 36 (currently amended): The method according to Claim 25, further comprising steps of:

obtaining a new value from the user to be used as the propagated identifying secret if the validation succeeds; and

substituting this new value for the identifying secret prior to operation of the propagating step.